L9: Entry 2 of 2 File: USPT Dec 5, 2006

DOCUMENT-IDENTIFIER: US 7146367 B2
TITLE: Document management system and method

PRIOR-PUBLICATION:

DOC-ID	DATE
US 20030217034 A1	November 20, 2003

Description Paragraph (58):
A transaction party may store documents in the repository at database 48 through its workstation 52. The transaction party may acquire the image through any suitable means, for example via a fax machine 56, a scanner 58 or through uploading an existing electronic document from another storage device.

Description Paragraph (67):
A "Company Maintenance" button 72 presents a company list screen shown in FIG. 6. The company list screen includes a line for each client entity (in the mortgage example, the lender, broker, etc.)registered with the primary system for storing and managing documents. To the left of each company name are five icons that enable the administrator to view and update system settings for each company. If the administrator activates an icon 74 for a listed company, the primary server 42 (FIG. 3) presents a screen shown in FIG. 7 that lists all users authorized to access documents stored for the company. As shown in FIG. 7, the system stores each user's first name, last name and a login name. A user logging into the system presents a user name that is a combination of its company name and the login name shown in FIG. 7. A User ID, which the system automatically creates when a user is added, is also listed, as is the user's email address. A "delete" icon 76 allows the administrator to delete the user from access to the client's documents. An icon 78 presents a screen by which the administrator may reset the user's password. In the presently-described embodiment, user information is stored by SITE SERVER, available from MICROSOFT CORPORATION. SITE SERVER is also responsible for authenticating all requests to the Web Server. For each user, the SITE SERVER database provides a Globally Unique Identifier (GUID) as the User ID, which can be subsequently used to store and retrieve information related to the user in the repository database. It should be understood, however, that the system could use any suitable user database and authentication sub-system, such as Active Directory from MICROSOFT CORPORATION.

Description Paragraph (69):
Returning to FIG. 7, activation of an icon 82 permits the administrator to change the information shown for that user in FIG. 7. The system presents a screen similar to that shown in FIG. 8, except that the current user information populates the property fields. After changing any information as desired, the administrator may activate an "update" button to modify the user information in the database and as shown on the screen in FIG. 7.

Description Paragraph (76):
Returning to FIG. 6, activation of an icon 88 for a given company displays a screen

(not shown) listing each of the views defined for that party's folders. As indicated above, each folder defined by a transaction party corresponds to a given transaction. When the administrator initially enters the transaction party in the database, the transaction party specifies one or more lists of document types it expects to handle in its transactions. The administrator defines these document type lists in the database in association with that party. Additionally, each party can define one or more folder views used to organize a folder's contents when presenting the folder's information to a user. For each view, the party provides one or more desired document groups. From each document type list, the party specifies which document types should be placed into which document type groups defined for each view and in which order the document types should be sorted within the respective groups. All of this information is stored by the administrator in the database in association with the transaction party.

Description Paragraph (94):
Referring again to FIG. 3, when a transaction party user accesses host system 40 from its work station 52 through Internet 46, client interface process 62 (FIG. 4) requests the user's user name and password. Each user name must be unique. In one embodiment, the user name is the user's name as indicated in FIG. 7 in combination with the name of the transaction party with which the user is associated. Passwords are assigned as described above. If the user provides a valid user name and password, the user interacts with the client interface to manage document image views and folders through various web pages as described herein.

Description Paragraph (95):
The client interface first presents the transaction party user with a folder search screen, as shown in FIG. 12, that lists each folder attribute (FIG. 9) applicable for searching that transaction party's folders. The screen provides a field for each attribute, and the user may provide entries to one or more fields as desired. To automatically enter the present date in the "Date Created" field, or to automatically enter the user's name in the "Created By" field, the user activates buttons provided to the right of those fields. Activation of the "search" button at the bottom of FIG. 12 presents a screen shown in FIG. 13 listing each of the folders meeting the attribute limitation entered by the user at FIG. 12. In the illustrated example, the search criteria were for all folders in which the mortgage applicant state was Georgia. Responsively to the request, the client interface creates and executes a query against database 48 (FIG. 3) and presents the screen shown in FIG. 13 to the user at its work station. The column titles in FIG. 13 represent the folder attributes defined for search results for the transaction party to which the user is associated. The user may sort the search results using the attributes by clicking on the desired column heading.

Description Paragraph (97):
"Open Folder," "Edit Properties," "Fax Coversheets" and "Scan Coversheets" icons provided to the left of each folder shown in FIG. 13 permit the user to access the folder, edit its properties and obtain fax or scan coversheets by which the user may add additional documents to the folder. Activation of the "Open Folder" icon 100 for a given folder produces a folder view screen as shown in FIG. 14. The folder view screen includes a folder attributes box 102, a notes box 104 and a document list box 106. Folder attributes box 102 displays the attributes established for the selected folder. If the user has sufficient authority, the user may change the folder attributes by activation of an "edit" button at the top of box 106 through a screen shown at FIG. 15. An "edit attribute" tab on a tool bar 105 shown in FIG. 14 also directs the user to the folder property screen shown in FIG. 15. This screen lists each attribute and, except for the creation date and creator fields, provides an edit box through which the user may change the attribute information. The system automatically fills the "Date Created" and "Created By" fields when the user initially creates the folder. The folder property screen also permits the user to define the folder security profile that is to be applied to the folder. A pull-down list 108 includes the name of each folder

security profile defined for the transacting party to which the user is associated, as described above with respect to FIG. 11. The "update" button saves the changed folder properties in the database, and a "reset" button removes any unwanted and unsaved edits from the current screen. To return to the folder view screen shown in FIG. 14, the user closes the window in which the folder properties screen is displayed.

Description Paragraph (104):
Within a folder, a user may instruct the client interface to send an email to the user's email address, or to other selected addresses, when the folder receives documents of a predefined type. To set such notifications in a folder, the user activates a "notifications" tab on toolbar 105. In response, the client interface presents a notifications screen as shown in FIG. 17. The notification screen includes a description line 116 in which the user may enter text to be included in the email message. In a pull-down list 118, the user may select any of the email addresses for users associated with the same transaction party, and/or the user may enter other email addresses at line 120. The user may select one or more document types that will trigger a notification in a box 122.

Description Paragraph (116):
The scan program code permits the user to scan images without a scanning coversheet. To do so, the user selects the "file" pull-down list from a main scan program page (FIG. 23) presented by the scan program at workstation 52 and selects a "Select Destination Folder" from the resulting pull-down menu. This causes the scan program code to produce a folder search screen at the user's workstation, as shown in FIG. 24. Upon filling in desired search criteria and activating a "search" button on the screen, the scan program code connects to the client interface at the host system and provides the search criteria to the client interface. The client interface executes appropriate queries against database 48 and returns a list of folders that meet the search criteria for the transaction party with which the user is associated, as shown in FIG. 25.

Description Paragraph (158):
Referring to table 172, FOLDER_DOCUMENTS, each document may be associated with one or more folders. As such, for each document associated with a folder, an entry is made in this table. The FOLDER_ID column identifies the folder with which the document is associated. The DOCUMENT_ID column identifies the document being associated. The DOC_TYPE column identifies the document's classification within the folder, and must be a valid member of the document type list associated with the folder. The TITLE column optionally indicates a title for the document. The COMMENTS column optionally indicates comments for the document. The SECURITY_ID column indicates the document security profile that is to be applied to the document. The ADDED_BY_USER_ID column indicates the individual user that associated the document with the folder. The ADDED_DATE indicates the date and time at which the document was associated with the folder. The VERIFIED_STATUS indicates whether the document has not been verified, as described previously in the discussion of the folder view web page (FIG. 14).

Description Paragraph (164):
Referring to table 190, FOLDERS_SECURITY_PROFILES_ROLE_MEMBERS, each user that will be granted any level of access to a folder must first be assigned to one of the roles defined by the security profile applied to that folder. For each such user, an entry must be made in this table. The SECURITY_ID and ROLE_ID columns indicate the profile and role with which the user will be associated. The USER_ID column indicates the user that is being associated.

Description Paragraph (167):
Referring to table 184, DOCUMENTS_SECURITY_PROFILES_ROLE_MEMBERS, each user that will be granted any level of access to a document must first be assigned to one of the roles defined by the security profile applied to that document. For each such

user, an entry must be made in this table. The SECURITY_ID and ROLE_ID columns indicate the profile and role with which the user will be associated. The USER_ID column indicates the user that is being associated.

CLAIMS:

15. A system for managing documents at an electronic data repository, where the documents relate to a transaction involving a plurality of parties having different roles in the transaction, the system comprising: an electronic data repository; and a computer program configured to receive a plurality of documents (received documents) from one or more parties of a plurality of parties that are involved in the transaction and that are remote from the repository and from each other, store the received documents in the repository, and for each first remote party of the plurality of remote parties, define, responsively to instructions from the first remote party, a document set corresponding to the first remote party, wherein the document set includes one or more predetermined types of the received documents, permit the first remote party access to said received documents that are within the document set corresponding to the first remote party, prohibit the first remote party from modifying any first document of the received documents in the repository, and from deleting the first document from the repository, while the first document is part of a document set of another remote party of the plurality of remote parties, and responsively to the first remote party, permit a second remote party of the plurality of remote parties access, in a document set corresponding to the second remote party, to first documents that are in the document set corresponding to the first remote party, and thereafter permit a third remote party of the plurality of remote parties access to the first documents responsively to the second remote party.

35. Within a transaction involving a plurality of parties having different roles in the transaction, a computerized method for managing documents related to the transaction and controlling access to the documents, the method comprising: receiving a plurality of documents (received documents) relating to the transaction from one or more parties of a plurality of parties that are involved in the transaction; storing the received documents in an electronic data repository, wherein said one or more parties are remote from the repository and from each other, wherein the documents are applied to one or more document sets corresponding to respective remote parties, and wherein each said document set includes one or more predetermined types of said received documents; and for each first remote party of the plurality of remote parties, providing the first remote party access to said received documents that are within a document set corresponding to the first remote party, prohibiting the first remote party from modifying any first document of the received documents in, and from deleting the first document from, the repository while the first document is part of a document set of another remote party of the plurality of remote parties, and permitting, responsively to the first remote party, a second remote party of the plurality of remote parties access, in a document set corresponding to the second remote party, to first documents in the document set corresponding to the first remote party, and thereafter permitting a third remote party of the plurality of remote parties access to the first documents responsively to the second remote party.

40. Within a transaction involving a plurality of parties having different roles in the transaction, a computerized method for managing documents related to the transaction and controlling access to the documents, the method comprising: (a) providing an electronic data repository; (b) receiving a plurality of documents (received documents) relating to the transaction from one or more parties of a plurality of parties remote from the repository and from each other and having a role in the transaction; (c) storing the received documents in electronic form in the repository; and (d) for each first remote party of the plurality of remote parties, defining a document set corresponding to the first remote party, wherein the document set includes one or more predetermined types of the received documents

and wherein the first remote party defines a categorization of the one or more predetermined of the received document types within the document set corresponding to the first remote party, providing each first remote party access to said received documents that are within the document set corresponding to the first remote party, organized by the categorization defined by the first remote party, prohibiting any first remote party from modifying any first document of the received documents in, and from deleting the first document from, the repository while the first document is part of a document set of another remote party of the plurality of remote parties, maintaining a map that defines a correspondence between the categorization of the one or more predetermined types of the received documents within the document set corresponding to a first remote party and the categorization of the one or more predetermined types of the received documents within a document set corresponding to a second remote party of the plurality of remote parties, following the maintaining step and responsively to the first remote party, applying one or more received first documents included in the document set corresponding to the first remote party to the document set corresponding to the second remote party according to the map, and responsively to the second remote party, applying the one or more received first documents to a document set corresponding to a third remote party of the plurality of remote parties.

43. A computer readable carrier including a computer program that causes a computer to manage and control access to documents at an electronic data repository used by a plurality of parties to a transaction, the computer program causing the computer to perform the steps of: (a) receiving a plurality of documents (received documents) from one or more parties of a plurality of parties remote from the repository and from each other; (b) storing the received documents in the repository in an electronic format; (c) for each first remote party of the plurality of remote parties, providing the first remote party access to received documents within a document set corresponding to first the remote party, wherein said document set includes one or more predetermined types of said received documents, prohibiting the first remote party from modifying any first document of the received documents in the repository, and from deleting the first document from the repository, while the first document is part of a document set of another remote party of the plurality of remote parties, and permitting, responsively to the first remote party, a second remote party of the plurality of remote parties access, in a document set corresponding to the second remote party, to first documents that are in the document set corresponding to the first remote party, and thereafter permitting a third remote party of the plurality of remote parties access to the second documents responsively to the second remote party.

Previous Doc Next Doc Go to Doc#